(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 February 2001 (15.02.2001)

PCT

(10) International Publication Number
WO 01/11817 A2

(51) International Patent Classification[7]: H04L 9/00

(21) International Application Number: PCT/US00/21414

(22) International Filing Date: 7 August 2000 (07.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/147,944	6 August 1999 (06.08.1999)	US
60/148,624	12 August 1999 (12.08.1999)	US
09/632,716	4 August 2000 (04.08.2000)	US

(71) Applicant: SARNOFF CORPORATION [US/US]; 201 Washington Road, CN 5300, Princeton, NJ 08543 (US).

(72) Inventor: WALDMAN, Harvey; 947 Pickering Drive, Yardley, PA 19067 (US).

(74) Agents: MOSER, Raymond, R., Jr et al.; Thomason, Moser & Patterson, LLP, 1st Floor, 595 Shrewsbury Avenue, Shrewsbury, NJ 07702 (US).

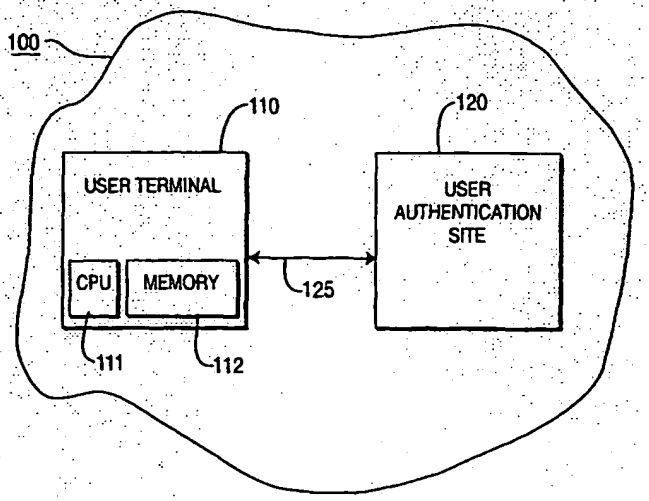
(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *Without international search report and to be republished upon receipt of that report.*

[Continued on next page]

(54) Title: NETWORK USER AUTHENTICATION PROTOCOL



(57) Abstract: In a network having a plurality of user terminals and a user authentication site, a method for authenticating a user. A user terminal of the network receives a password from a user, and translates the password into an authentication encryption key for the user. The terminal generates a first random number, encrypts the first random number with the authentication encryption key to provide a first encrypted message, and transmits the first encrypted message to the user authentication site. The user authentication site decrypts the encrypted first message to provide the first random number, and generates a second random number, which is transmitted to the user terminal. The user terminal combines and encrypts the first and second random numbers, with the authentication encryption key, to provide a second encrypted message. The user terminal transmits the second encrypted message to the user authentication site, which decrypts the encrypted second message to provide the combined first and second random numbers. The user authentication site verifies that the first and second random numbers are correct, and authenticates the user in accordance with this verification.

WO 01/11817 A2

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

NETWORK USER AUTHENTICATION PROTOCOL

CROSS-REFERENCES TO RELATED APPLICATIONS

This nonprovisional U.S. national application, filed under 35 U.S.C. §111(a), claims, under 37 C.F.R. §1.78(a)(3), the benefit of the filing date of provisional U.S. national application no. 60/147,944, attorney docket no. SAR-13276P, filed on 08/06/99 under 35 U.S.C. §111(b), the entirety of which is incorporated herein by reference, and the benefit of the filing date of provisional U.S. national application no. 60/148,624, attorney docket no. SAR13431P, filed on 08/12/99 under 35 U.S.C. §111(b), the entirety of which is incorporated herein by reference.

GOVERNMENT INTERESTS

This invention was at least partially supported by U.S. Army CECOM Government Contract No. DAAB07-97-C-D607. The government may have certain rights in this invention.

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to computer networks and, in particular, to systems and methods for authentication of users seeking access to the network.

Description of the Related Art

Computer networks are widely used. These include private networks such as local-area networks ("LANs"), wide-area networks ("WANs"), and the Internet. The network consists of a variety of nodes, interconnected by transmission media. Some nodes may be terminals and/or personal computers ("PCs") by which a user gains access to the network. Other network nodes are functional units such as routers, servers, and the like. Various communications media are used to interconnect the nodes of a network, such as fiber-optic cables, Integrated Services Digital Network ("ISDN"), wireless links, and the like. As will be understood, various nodes of a networked computer system may be connected through a variety of communication media.

A given private network is typically maintained and operated by a specific company, where access to the network is limited to authorized users. In order to limit access to authorized users, networks are often configured to "authenticate" a user attempting to access the network, to ensure that the user is an authorized user. The authentication procedure is thus designed to ensure that only authorized (authenticated) users are allowed to access the network. The simplest form of authentication requires a username or user ID, and password to gain access to a particular account. Authentication protocols can also be based on secret-key encryption or on public-key systems using digital signatures. In some networks, in order to maintain network access control, users are required to be periodically re-authenticated to retain network access. The authentication process authenticates an authorized user. The outcome of the authentication can be said to be successful if the user is successfully authenticated, i.e. authorized to access the networl. The authentication fails if the user is not granted authorization to access the network.

Conventional authentication procedures, however, may be subject to infiltration by unauthorized users, or other forms of "attack". The attack may permit substitute or false information to be inserted into the network, or delivered from the network, or it may otherwise permit the unauthorized user to gain access to the network, further allowing them to perform a range of hostile acts. If authentication information resides in the memory of a network terminal, whether mobile, wireless, or fixed, it may be possible for an unauthorized user to attack the memory to acquire the authentication information, and thus access to the system.

For example, in a network with mobile users (i.e., wireless, mobile terminals), there may be opportunity for user terminals to fall into unauthorized hands in which the terminal memory may be attacked. If the hacker acquires authentication information stored in the memory of the terminal, this may be used to gain unauthorized access of the network. Also, some networks and authentication procedures are vulnerable to so-called "man-in-the-middle" attacks. In this kind of an attack, an unauthorized user interferes with the initial public key exchange, by intercepting the very first

message to a new correspondent (e.g., from the terminal to some authentication server of the network) and substituting a bogus public key for the genuine public key. There is, therefore, a need for improved authentication systems and techniques which do not suffer the foregoing disadvantages and problems.

SUMMARY

In a network having a plurality of user terminals and a user authentication site, a method for authenticating a user. A user terminal of the network receives a password from a user, and translates the password into an authentication encryption key for the user. The terminal generates a first random number, encrypts the first random number with the authentication encryption key to provide a first encrypted message, and transmits the first encrypted message to the user authentication site. The user authentication site decrypts the encrypted first message to provide the first random number, and generates a second random number, which is transmitted to the user terminal. The user terminal combines and encrypts the first and second random numbers, with the authentication encryption key, to provide a second encrypted message. The user terminal transmits the second encrypted message to the user authentication site, which decrypts the encrypted second message to provide the combined first and second random numbers. The user authentication site verifies that the first and second random numbers are correct, and authenticates the user in accordance with this verification.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other features, aspects, and advantages of the present invention will become more fully apparent from the following description, appended claims, and accompanying drawings in which:

Fig. 1 is a block diagram of a computer network in accordance with an embodiment of the present invention; and

Fig. 2 is a flow chart illustrating the authentication protocol of the network of Fig. 1, in accordance with an embodiment of the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention provides an authentication protocol designed to prevent unauthorized entities from gaining access to the network either by obtaining authentication information through communications attack or by gaining access to a network terminal. In the present invention, only information personally retained by an authorized user may be used for authentication. No authentication information resides in any user's terminal, thereby minimizing the risk of an unauthorized user gaining access through a terminal, such as a mobile terminal. In addition, the authentication protocol of the present invention is not susceptible to a man-in-the-middle attack.

Referring now to Fig. 1, there is shown a block diagram of a computer network system 100 in accordance with an embodiment of the present invention. Network 100 includes a user terminal 110, and a user authentication site 120, interconnected by a communications or transmission channel 125, which may be a LAN, fiber optic, wireless, or other digital communications means. User terminal 110 may be a PC at a fixed location, a remote PC connected to authentication site 120 by a telephone or other link, or a mobile unit connected by a wireless link. Terminal 110 contains a processor (CPU 111) and memory 112. User authentication site 120 may be a server or other dedicated piece of hardware, a PC, or even a site manned by human operators. There may be more than one authentication site in network 100.

Each authorized user of network 100 is assigned a unique password, and an authentication encryption and decryption key pair. A given user's authentication encryption key is the outcome of applying a specified encryption-key generation algorithm to the user's password. The user's authentication decryption key is the key that can decrypt messages encrypted using the user's authentication encryption key. These keys are used only for authentication and no other purpose, such as data encryption/decryption. Only the user authentication site(s) 120 stores the user's authentication encryption and decryption keys, password, and other information about the user, such as the user's security clearance, authority to access the network

(access authority). No user terminal stores the user's encryption or decryption keys, or the user's password (except for temporarily storing the user's password and authentication encryption key during the authentication process).

In some embodiments, each user may also have a Smart Card with personal information pre-encrypted with the user's individual authentication encryption key. Each user may also have health sensors mounted on his body, for additional security.

Each user terminal, such as user terminal 110, has a means of translating the user's password to the user's individual encryption key. For example, user terminal 110 contains processor 111 and the above-mentioned encryption-key generation algorithm. User terminal 110 also has the ability to generate random numbers, and to encrypt a given message with the user's individual authentication encryption key. Thus, if the user provides a password to terminal 110, terminal 110 can run the encryption-key generation algorithm using the password as input, to generate the user's authentication encryption key. It can then generate a random number and use the authentication encryption key to encrypt the random number, to provide an encrypted random number (which is also a random number). The password, random number, authentication encryption key, encrypted messages, and received messages, can be stored by terminal 110 temporarily in memory 112. In some embodiments, a terminal 110 can be equipped with sensors to read and transmit the user's Smart Card information, health sensors, and/or an iris recognition device, for additional security.

Referring now to Fig. 2, there is shown a flow chart illustrating the network user authentication protocol method 200 of network 100, in accordance with an embodiment of the present invention. First, a user initiates access of a user terminal 110 (step 201). Alternatively, if a user has been using a given terminal 110 for some time, after a timeout, authentication site 120 notifies user terminal 110 to re-authenticate the user (step 203). Terminal 110 then notifies the user to enter a user ID and password, for example within a given time period (step 205). In the case of re-authentication, step 205 may involve issuing an Authentication Warning

to the user, which may be in the form of a visual, auditory, or skin sensation message. Also, in the case of re-authentication in which the user is currently engaged in a session, the terminal 110 may still have user ID stored, in which case it need only prompt the user for the password.

The user presumably will only have a password if he is an authorized user. In this case, the authorized user enters his user ID and password (step 207), within a specified timeout period if this is required in step 205. Terminal 110 then generates the user's authentication encryption key by translating the password into this key with the encryption-key generation algorithm (209). Thus, the user need not ever possess or even know his authentication encryption key, but only his password (and ID).

Terminal 110 also generates a first random number (step 211), and then encrypts this random number using the user's authentication encryption key (step 213). The user terminal then notifies the user authentication site 120 of the user's identity and transmits the encrypted random number to user authentication site 120 (step 215). In an embodiment, the authentication site is notified of the user's identity by transmitting the user ID to the authentication site. The user ID is preferably first encrypted with the user's authentication encryption key and then the encrypted ID is transmitted to authentication site 120. Authentication site 120 can then exhaustively decrypt the received encrypted message, with every possible authentication decryption key, until there is produced a user ID which matches a valid user ID of the network (and which also matches the user ID of the decryption key used to successfully decrypt the message). Thus, once authentication site 120 has successfully decrypted the user ID message, it knows the user ID and thus which authentication decryption key to use to decrypt subsequent encrypted messages transmitted during the authentication process. In an embodiment, the user terminal 10 ID is also encrypted and transmitted to authentication site 120 along with the user ID. In the case of re-authentication, the encrypting and sending of the user ID can be skipped; or, for convenience and simplicity, it can still be transmitted, but the authentication site 120 can in this case simply use the already-

determined decryption key to decrypt the encrypted user ID, rather than perform an exhaustive decryption.

After decrypting the encrypted user ID message, authentication site 120 receives the encrypted first random number. User authentication site 120 decrypts this message with the particular user's authentication decryption key, to provide the original first random number (step 217). User authentication site 120 then generates a second random number, and transmits it to user terminal 110 (step 219). In an alternative embodiment, an encrypted version of the second random number is transmitted to user terminal 110, in which a second encryption/decryption key pair is utilized.

At this point in time, user authentication site 120 knows the identity of the user and/or his password, that user's authentication encryption/decryption keys (or at least the decryption key), and the first and second random numbers. The user terminal 110 only temporarily, during the authentication process, stores the user's password and authentication encryption key.

After receiving the second random number from authentication site 120, the user's terminal 110 combines and encrypts both random numbers with the user's authentication encryption key and transmits this message to the user authentication site (step 221). The two random numbers may be combined in a variety of specified ways, e.g. adding, subtracting, multiplying, concatenating strings, and so forth, so long as the technique used by user terminal 110 is known to user authentication site 120. The combining technique used is preferably set apriori and specified as part of the authentication protocol of the present invention.

The user authentication site 120 thus receives an encrypted message, which is an encrypted version of the combined two random numbers, and decrypts this message using the user's authentication decryption key. Authentication site 120 then verifies that both random numbers are correct. If so, there has been no man-in-the-middle attack. At this point, authentication site 120 knows the identify of the user attempting to gain access. If the user's identify and access authority permit network access, authentication site 120 authenticates the user by transmitting the appropriate

authentication message to terminal 110 and allowing network resources to be used by the user from user terminal 110, in accordance with the user's level of access authority (step 223). If the user is a new user, he is authenticated, or denied access if the authentication fails. In the case of re-authentication, the user is re-authenticated, or authentication is withdrawn if the authentication fails.

In an alternative embodiment, user authentication site 120 may also query user terminal 110 for Smart Card information, the status of the user's health, and/or iris recognition information. This information may be used for additional security by authentication site 120, in step 223, in verifying the user's identity and ability to conduct a terminal session. Whether authentication fails or is successful, the user terminal 110 in both cases erases the user's password and authentication encryption key from its memory 112 immediately after the authentication process is completed (step 225).

As will be understood, the term "user" as used herein refers to a person either attempting to gain access, or already having access, to the network 100 via a user terminal 110. Thus a prospective user as well as one already authorized by an authentication process is a user.

In an embodiment, health sensors are also provided. If at any time during a session user terminal 110 detects that the user is unable to conduct a terminal session, based on status from the health sensors, this information is transmitted to the user authentication site 120 and the latter withdraws authentication.

As will be appreciated, the authentication protocol of the present invention is not vulnerable to a man-in-the-middle attack. Further, authentication data security is attained by not permitting individual authentication information to reside on any user terminal 110. Limiting user authentication information to the user authentication site 120 attains user security. Further, having user authentication site 120 control access to user terminal 110 attains terminal access and security.

It will be understood that various changes in the details, materials, and arrangements of the parts which have been described and illustrated

above in order to explain the nature of this invention may be made by those skilled in the art without departing from the principle and scope of the invention as recited in the following claims.

What is claimed is:

1. In a network (100) having a plurality of user terminals (110) and a user authentication site (120), a method (200) for authenticating a user, comprising the steps of:

(a) receiving (207), at a user terminal (110) of the network (100), a password from a user;

(b) translating (209) the password into an authentication encryption key for the user; and

(c) using (211-225) the authentication encryption key to authenticate the user with the user authentication site (120).

2. The method of claim 1, wherein step (c) comprises the steps of:

(1) generating (211), with the user terminal, a first random number;

(2) encrypting (213) the first random number with the authentication encryption key to provide a first encrypted message and transmitting (215) the first encrypted message from the user terminal to the user authentication site;

(3) decrypting (217), at the user authentication site, the encrypted first message to provide the first random number;

(4) generating (219), with the user authentication site, a second random number and transmitting the second random number to the user terminal;

(5) combining and encrypting (221), with the user terminal, the first and second random numbers to provide a second encrypted message and transmitting the second encrypted message from the user terminal to the user authentication site;

(6) decrypting (223), at the user authentication site, the encrypted second message to provide the combined first and second random numbers;

(7) verifying (223) that the first and second random numbers are correct; and

(8) authenticating (223) the user in accordance with said verification.

3. The method of claim 2, comprising the further step of erasing (225) from the user terminal the password after the user authentication, whether the authentication is successful or not.

4. The method of claim 2, wherein:

step (a) comprises the further step of receiving (207)), at the user terminal, a user ID from the user;

step (c)(2) comprises the further step of encrypting the user ID with the authentication encryption key to provide an encrypted user ID message and transmitting (215) the encrypted use ID message from the user terminal to the user authentication site; and

step (c)(3) comprises the further step of decrypting, at the user authentication site, the encrypted user ID message with valid authentication decryption keys until a decrypted user ID is produced which matches a valid user ID of the network, step (c)(3) further comprising the step of decrypting the encrypted first message with the authentication decryption key used to successfully decrypt the encrypted user ID message, to provide the first random number.

5. The method of claim 2, wherein step (c)(8) comprises the step of authenticating (223) the user if the first and second numbers are correct and if the user has authority to access the network.

6. The method of claim 2, further comprising the steps of reading, with a health sensor, the user's health status, transmitting said health status to the user authentication site, and authenticating the user in accordance with said health status and said verification of step (c)(7).

7. The method of claim 2, further comprising the steps of querying, with the authentication site, the user terminal to read user information from a user smart card and authenticating the user in accordance with said user information and said verification of step (c)(7).

8. The method of claim 1, wherein step (a) comprises the steps of:

notifying (205) the user, with the terminal, to enter a user ID and the password when one of (1) a new user initiates (201) access of the terminal and (2) the authentication site notifies (203) the terminal when being used to re-authenticate after a time-out; and

receiving, at the user terminal, the user ID from the user.

9. In a network (100) having a plurality of user terminals (110), a method for encrypting data, comprising the steps of:

(a) receiving (207), at a user terminal (110) of the network (100), a network password from a user;

(b) translating (209), with an encryption-key generation algorithm, the password into an authentication encryption key for the user; and

(c) using the authentication encryption key to encrypt (213) data to provide an encrypted message.

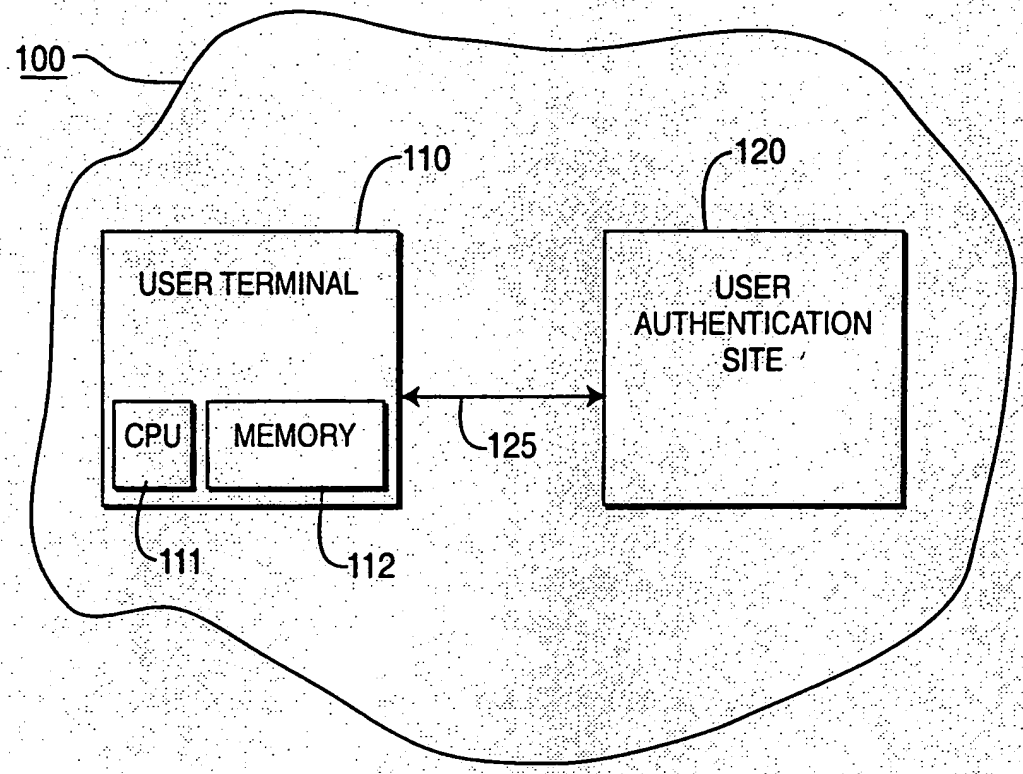

100
110
120
USER TERMINAL
USER AUTHENTICATION SITE
CPU
MEMORY
125
111
112

FIG. 1

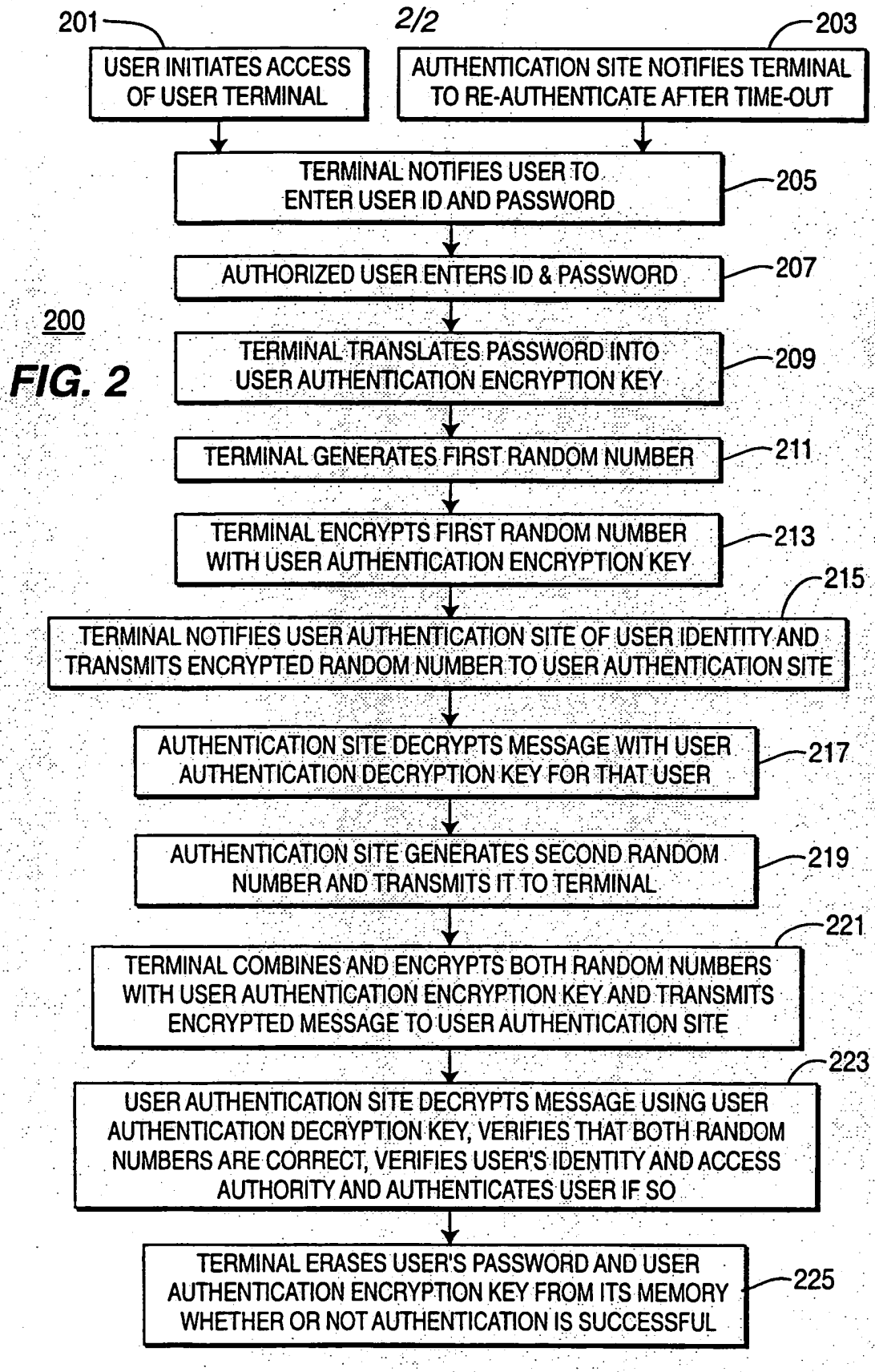

201
USER INITIATES ACCESS OF USER TERMINAL
203
AUTHENTICATION SITE NOTIFIES TERMINAL TO RE-AUTHENTICATE AFTER TIME-OUT
TERMINAL NOTIFIES USER TO ENTER USER ID AND PASSWORD
205
AUTHORIZED USER ENTERS ID & PASSWORD
207
200
TERMINAL TRANSLATES PASSWORD INTO USER AUTHENTICATION ENCRYPTION KEY
209
TERMINAL GENERATES FIRST RANDOM NUMBER
211
TERMINAL ENCRYPTS FIRST RANDOM NUMBER WITH USER AUTHENTICATION ENCRYPTION KEY
213
215
TERMINAL NOTIFIES USER AUTHENTICATION SITE OF USER IDENTITY AND TRANSMITS ENCRYPTED RANDOM NUMBER TO USER AUTHENTICATION SITE
AUTHENTICATION SITE DECRYPTS MESSAGE WITH USER AUTHENTICATION DECRYPTION KEY FOR THAT USER
217
AUTHENTICATION SITE GENERATES SECOND RANDOM NUMBER AND TRANSMITS IT TO TERMINAL
219
221
TERMINAL COMBINES AND ENCRYPTS BOTH RANDOM NUMBERS WITH USER AUTHENTICATION ENCRYPTION KEY AND TRANSMITS ENCRYPTED MESSAGE TO USER AUTHENTICATION SITE
223
USER AUTHENTICATION SITE DECRYPTS MESSAGE USING USER AUTHENTICATION DECRYPTION KEY, VERIFIES THAT BOTH RANDOM NUMBERS ARE CORRECT, VERIFIES USER'S IDENTITY AND ACCESS AUTHORITY AND AUTHENTICATES USER IF SO
TERMINAL ERASES USER'S PASSWORD AND USER AUTHENTICATION ENCRYPTION KEY FROM ITS MEMORY WHETHER OR NOT AUTHENTICATION IS SUCCESSFUL
225

FIG. 2